Sub A2

1. A method for brokering state information exchanged between computers using at least one protocol above a transport layer, the method comprising the steps of:

receiving at a proxy a request from a client requesting a resource of an origin server;

redirecting the client request from the proxy to a policy module;

obtaining at the proxy policy enforcement data provided by the policy module;

generating at the proxy a policy state token in response to the policy enforcement data; and

transmitting the policy state token from the proxy to the client.

2. The method of claim 1, further comprising the step of receiving at the proxy a renewed request for the origin server resource, the renewed request containing the policy state token.

3. The method of claim 2, wherein the renewed request contains the policy state token in a cookie in a header sent from the client to the proxy.

4. The method of claim 2, further comprising the step of forwarding to the origin server a portion of the renewed request, the forwarded portion omitting the policy state token.

5. The method of claim 4, further comprising the step of receiving at the proxy a reply from the origin server, the reply containing an origin state token for use by the proxy in its subsequent communications with the origin server.

6. The method of claim 4, further comprising the steps at the proxy of forwarding to the client at least a portion of a communication from the origin server, and forwarding to the origin server at least a portion of a communication from the client.

7. The method of claim 1, wherein HTTP is a protocol used during at least one of the receiving and transmitting steps.

A2

8. The method of claim 1, wherein HTTPS is a protocol used during at least one of the receiving and transmitting steps.

9. The method of claim 1, wherein the method further comprises utilizing Novell Directory Services software to provide authentication information about the client, and the policy enforcement data obtained by the proxy depends on the authentication information thus provided.

10. The method of claim 1, wherein the method further comprises utilizing Lightweight Directory Access Protocol software to provide authentication information about the client, and the policy enforcement data obtained by the proxy depends on the authentication information thus provided.

11. The method of claim 1, wherein the method further comprises utilizing Secure Sockets Layer software to provide authentication information about the client, and the policy enforcement data obtained by the proxy depends on the authentication information thus provided.

12. The method of claim 1, wherein the obtaining step extracts policy enforcement data from a redirection address field.

13. The method of claim 1, wherein the transmitting step transmits the policy state token in a cookie in a header sent from the proxy to the client.

A2

14. A transparent proxy server comprising:

a memory configured at least in part by a transparent proxy process;

a processor for running the transparent proxy process;

at least one link for networked communication between the transparent proxy process, on the one hand, and a client computer and an origin server, on the other hand; and

a policy module identifier which identifies a policy module that grants or denies authorization of proxy services.

15. The transparent proxy server of claim 14, in combination with the policy module.

16. The transparent proxy server of claim 15, wherein the policy module and the transparent proxy process are running on the same computer.

17. The transparent proxy server of claim 14, in combination with the client computer and at least one other client computer, each client computer linked for networked communication with the transparent proxy process.

18. The transparent proxy server of claim 14, wherein the transparent proxy server provides authorized proxy service transparently to both a client computer and an origin server by steps which comprise receiving a request from the client for a resource of the origin server, sending the client an authorization by the policy module for the client to use a transparent proxy service, accepting the authorization from the client with a renewed client request for the origin server resource, forwarding the renewed client request to the origin server without forwarding the authorization but with an indication to the origin server that the transparent proxy server is the source of the forwarded request, and then transparently forwarding the requested resource from the origin server to the client.

A2

19. The transparent proxy server of claim 18, wherein the transparent proxy server sends the client the authorization by sending the client a proxy cookie for use in subsequent communications from the client.

20. The transparent proxy server of claim 14, in combination with at least one additional transparent proxy server which also has a memory configured at least in part by a transparent proxy process, a processor for running the transparent proxy process, a link, and a policy module identifier.

21. The combined transparent proxy servers of claim 20, wherein one transparent proxy server forwards client requests to the other transparent proxy server.

22. The combined transparent proxy servers of claim 20, wherein one transparent proxy server takes over the handling of client requests in place of the other transparent proxy server.

23. A pair of state information brokering signals embodied in a distributed computer system, the system containing a client, a transparent proxy server having a transparent proxy server address, and a policy module having a policy module address, the pair of signals comprising:

A2

a first signal including a redirection command which specifies the policy module address as a redirection target; and

a second signal including a redirection command which specifies the transparent proxy server address as a redirection target and also including policy enforcement data which grants or denies authorization for the client to use a service of the transparent proxy server.

24. The signal pair of claim 23, wherein the first signal includes an identity broker address as the policy module address.

25. The signal pair of claim 23, wherein the first signal includes a login server address as the policy module address.

26. The signal pair of claim 23, wherein the second signal includes the policy enforcement data embedded in an address field with the transparent proxy server address.

27. A computer storage medium having a configuration that represents data and instructions which will cause performance of method steps for transparent proxy services, the method comprising the steps of:

receiving at a transparent proxy a request from a client requesting a resource of an origin server;

A2

redirecting the client request from the transparent proxy to a policy module; and

obtaining at the transparent proxy policy enforcement data provided by the policy module, the policy enforcement data granting or denying authorization for the client to access the resource through the transparent proxy.

28. The configured storage medium of claim 27, wherein the policy enforcement data grants authorization for the client to access the resource through the transparent proxy, and the method further comprises the steps of generating at the transparent proxy a proxy cookie containing at least a portion of the policy enforcement data, and transmitting the proxy cookie from the transparent proxy to the client.

29. The configured storage medium of claim 28, wherein the method further comprises the steps of accepting the proxy cookie at the transparent proxy with a renewed client request for the origin server resource, and forwarding the renewed client request to the origin server without the proxy cookie.

30. The configured storage medium of claim 29, wherein the method further comprises the step of transparently forwarding the requested resource from the origin server to the client.

31. The configured storage medium of claim 27, wherein the transparent proxy is a first transparent proxy, the policy enforcement data includes first policy enforcement data which grants authorization for the client to access the resource through the first transparent proxy, and the method further comprises the steps of:

generating at the first transparent proxy a proxy cookie in response to the first policy enforcement data;

A2

transmitting the proxy cookie from the first transparent proxy to the client;

receiving the first proxy cookie from the client at a second transparent proxy with a renewed client request for the origin server resource, after the first transparent proxy becomes unavailable to the client;

redirecting the renewed client request from the second transparent proxy to a policy module; and

accepting, at the second transparent proxy, second policy enforcement data provided by the policy module, the second policy enforcement data including authorization from the policy module for the client to access the resource through the second transparent proxy.